

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-14239
(P2001-14239A)

(43) 公開日 平成13年1月19日 (2001.1.19)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 1 7
12/14	3 1 0	12/14	3 1 0 A 5 B 0 8 5
			3 1 0 K 5 B 0 8 9
15/00	3 2 0	15/00	3 2 0 A

審査請求 未請求 請求項の数 8 O L (全 9 頁)

(21) 出願番号 特願平11-182908

(22) 出願日 平成11年6月29日 (1999.6.29)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 古川 博

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 篠原 大輔

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

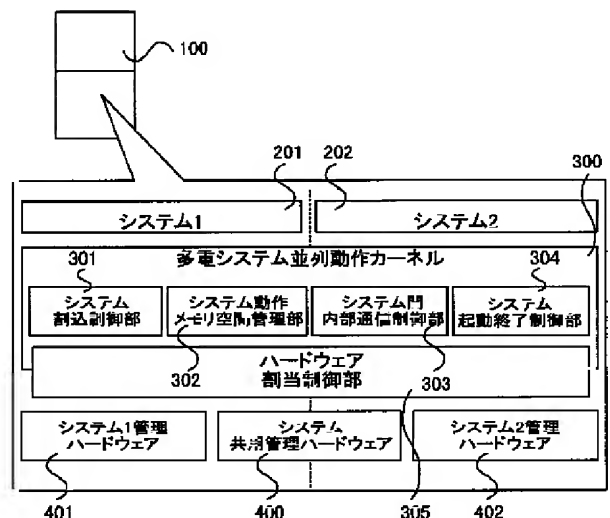
(54) 【発明の名称】 多重システム並列稼働計算機によるセキュリティシステム

(57) 【要約】

【課題】主たる課題は、単一計算機上で複数システムを同時並列稼働させる環境を利用し、同時並列稼働しているシステム同士のセキュリティをシステム自体の改造をすることなく確保する。

【解決手段】一台の計算機上で動作する1つのシステムが他のシステムに影響を及ぼさないセキュリティがシステム自体を改造無しで実現可能とし、公共回線先のクライアントから特定サイト内へアクセスをする際の高度な通信制御セキュリティ機能を提供する中継器のシステムとして利用可能である。

図1



【特許請求の範囲】

【請求項1】 一台の計算機上で複数のシステムを同時並列稼働する計算機で、少なくとも一つのシステムである監視システムが中心になり、他のシステムとシステム間通信により情報を受け渡しする環境において、前記監視システムが、少なくとも他のシステムとのシステム間通信の内容、認証情報、および他のシステムからの不正なシステム間通信制御の監視を行い、前記監視システム以外で不正な侵入や不正な制御が行われたことを前記監視システム検知した場合には、少なくとも前記監視システムには不正の侵入、制御の影響が及ばないことを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。

【請求項2】 請求項1において、一台の計算機上で動作する複数のシステム動作環境は、全く独立した環境で動作することを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。

【請求項3】 請求項1において、一台の計算機上で動作する複数のシステムは、計算機起動時に一台の計算機上に存在するハードウェアを、各々が管理するハードウェアとして割当が可能であることを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。

【請求項4】 請求項1において、一台の計算機上で動作する複数のシステム間の通信は、機器内部のシステム間通信により可能であり、前記機器内部のシステム間通信にはアクセス制限が設定可能であることを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。

【請求項5】 請求項1において、一つのシステムに不正な侵入や不正な制御が行われた場合、機器電源のリセット無しに、前記不正侵入、制御が行われたシステムのみ終了、リセットし、他のシステムには影響が及ばないことを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。

【請求項6】 少なくとも公共回線経由で、通信制御を行うシステムの一台の中継用計算機に、請求項1の複数のシステムが同時並列稼働する計算機を使用し、前記複数のシステムの内1つが監視システムとなり他のシステムを監視し、監視システムは内部の回線に、他のシステムは外部の公共回線に、それぞれ接続した環境を提供し、前記提供された環境は、請求項1、2、3、4、5の特長を利用することにより、少なくとも公共回線に接続するシステムに外部からの不正な侵入、制御、攻撃が行われた場合にでも、内部の回線内には前記不正な侵入、制御、攻撃の影響が及ばない、安全の環境が提供可能であることを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。

【請求項7】 請求項6の公共回線は、少なくともインターネット、イントラネット、エクストラネットを含むことを特徴とする、多重システム並列稼働計算機によるセキ

ュリティシステム。

【請求項8】 請求項6の中継用計算機には、少なくともファイアウォール、パケット変換器を含むことを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、単一計算機上で複数のシステムを同時並列稼働することが可能な計算機により提供されるセキュリティシステムに関する。

【0002】 特にインターネット、イントラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークにおいて、前記公共回線上のクライアントから特定サイト内へアクセスをする際の通信制御セキュリティを少なくとも含む。

【0003】

【従来の技術】 従来、単一計算機上ではハードウェアを一元制御するため、1つのシステムが動作するのが一般的であった。また例え、複数のシステムを稼働する場合でも、特開平7-129419号の様に仮想的計算機として動作させ、ハードウェア制御/資源管理は仮想計算機のベースシステムが全てを実行していた。そのため、ベースシステムへの不正な侵入/操作などにより容易にセキュリティが破られる可能性が高かった。

【0004】 特にインターネット、イントラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークで、前記公共回線上のクライアントから特定サイト内へアクセスをする際の通信制御においては、単一のシステム、もしくは単一システム機器同士を組み合わせるなどした計算機器類を、通信制御用のセキュリティ中継器として使用することが一般的であった。つまり前記中継器用計算機のセキュリティ確保が同システムでの重要な課題であった。

【0005】

【発明が解決しようとする課題】 本発明では、単一計算機上で複数システムを同時並列稼働させる環境を利用し、同時並列稼働しているシステム同士のセキュリティをシステム自体の改造をすることなく確保する。本発明によれば、互いのシステム同士のセキュリティは、ベースで動く独自の多重システム並列稼働カーネルと前記多重システム並列稼働カーネルを制御する監視システムが受け持ち、1つのシステムに不正な侵入がされた場合でも、他のシステムに影響がないセキュリティを提供する。また、例え1つのシステムに外部から侵入し、前記カーネル経由で不正アクセスを試みられた場合でも、その操作を監視システムが確認した時点でアクセスを行ったシステム自身を終了するなど、他のシステムへの二次的な影響を防止する環境の提供も目的とする。

【0006】 特に前記のセキュリティを利用することで、現在飛躍的に増大しているインターネット、イント

ラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークにおいて、前記公共回線先のクライアントから特定サイト内へアクセスをする際の通信制御セキュリティ機能を提供することも、少なくとも一つの目的である。具体的には、前記通信制御で現在一般的に利用されている中継器用計算機に、前記複数のシステムが同時並列動作可能な計算機を利用し、セキュリティ確保をすることにより実現する。

【0007】

【課題を解決するための手段】上記課題を実現するための手段を、図1を用い説明する。

【0008】本発明は第一に、一台の計算機上で複数のシステムを同時並列稼働させる手段を有する。図1の300多重システム並列稼働カーネルが前記手段を提供する。具体的には、301システム割込制御部が、各システム間での割込を制御し、プロセッサの割当てやスケジューリングを行う。また、302システム動作メモリ空間管理部が各システムのメモリを管理し、各システム毎のメモリ割当てを行う。つまり多重システム並列稼働カーネル(300)は各システムの完全に制御可能であり、1つのシステムから多重システム並列稼働カーネル(300)へ不正アクセスが行われる場合には、304システム起動終了制御部を使って、汎用システム自体の停止も可能となる。

【0009】第二に、一台の計算機上に存在し、システム毎に独自管理しているハードウェアを他のシステムから隠蔽する手段を有する。図1の305ハードウェア割当制御部が前記手段を提供する。ハードウェア割当制御部(305)は、各システムが独自に管理するハードウェア(401および402)やシステムが共用で持つハードウェア(400)を管理し、起動時に各ハードウェアを各システムに割当てる機能を有し、前記機能により一方のシステムが有するハードウェアを他のシステムから分離し、隠蔽する事が可能となる。

【0010】第三に、一台の計算機上で同時並列稼働する複数のシステム間での通信を制御する手段を有する。図1の300多重システム並列稼働カーネル内の303システム間内部通信制御部は、ネットワークなど計算機外部への通信無しで、独自にお互いのシステム間の通信する機能を提供し、必要によりシステム間の通信にアクセス制限を設ける機能も提供可能である。

【0011】以上の手段を用い、一台の計算機上で動作する1つのシステムが他のシステムに影響を及ぼさないセキュリティがシステム自体の改造無しで実現可能であり、公共回線先のクライアントから特定サイト内へアクセスをする際の高度な通信制御セキュリティ機能を提供する中継器のシステムとして利用可能である。

【0012】

【発明の実施の形態】本発明の一実施例を、図面を用い

て説明する。

【0013】図1は、本発明のシステム構成を説明した図である。100は一台の計算機である。201、202は計算機(100)上で動作するシステムであり、少なくとも世の中に存在するオペレーティングシステム(OS)、ミドルソフトを含む計算機制御用ソフトウェアである。300は計算機(100)上で動作する多重システム並列動作カーネルであり、前記システム(201、202)を一台の計算機上で複数動作させるためのシステムである。多重システム並列動作カーネル(300)内には、301システム割込制御部、302システム動作メモリ空間管理部、303システム間内部通信制御部、304システム起動終了制御部が存在する。また、多重システム並列動作カーネル(300)内には、計算機内に存在するハードウェアを管理し、各システム毎のハードウェア割当てを可能にする、305ハードウェア割当制御部の一機能が存在する。401はシステム1(201)によって管理されている計算機(100)内のハードウェアであり、402は汎用システム2(202)によって管理されている計算機(100)内のハードウェアである。一方、400は計算機(100)内に存在する全てのシステムが共用で使用するハードウェアである。なお、本実施例では説明を簡単にするため、一台の計算機(100)内で動作するシステムは2つとしたが、これらは複数存在することが可能である。

【0014】多重システム並列動作カーネル(300)は、計算機(100)起動時に立ち上がり、複数のシステム(201、202)を動作させるための環境を整備する。302システム動作メモリ空間管理部が、各システム毎に必要なメモリ空間の割当てを行い、割当てられたメモリ空間上でそれぞれのシステムがロード可能になる。また、301システム割込制御部は、各システムが使用するプロセッサの割当てを起動時に行う。無論この割当ては複数のプロセッサが計算機(100)内に存在する場合であり、1つのプロセッサしかない場合は、システム割込制御部(301)が起動後プロセッサの割込スケジューリングを管理し、必要に応じ各システムに処理を渡すように制御を行う。

【0015】以上の様にして、一台の計算機上で複数のシステムが同時並列かつ独立して、しかもシステム自体に変更や改造を加えることなく動作可能になる。

【0016】またハードウェア割当制御部(305)も、多重システム並列動作カーネル(300)の一部として計算機(100)起動時に機能し、各システムが独自に管理するハードウェア(401、402)、共用で使用するハードウェア(400)の割当てを行う。起動後ユーザがアクセス可能なシステム(201、202)から、ハードウェアの情報取得した場合、システム1(201)からはシステム1管理ハードウェア(401)とシステム共用管理ハードウェア(400)が、システム2(202)からはシス

テム2管理ハードウェア(402)とシステム共用管理ハードウェア(400)が取得可能である。つまり自システムが管理していないハードウェア情報、システム1(201)ではシステム2管理ハードウェア(402)、システム2(202)ではシステム1管理ハードウェア(401)の情報は、その存在すら検知できないようになる。

【0017】以上説明してきた機能を利用することで、まったく独立した複数の計算機環境を一台の計算機上に実現可能である。

【0018】多重システム並列動作カーネル(300)は、その上で動作する複数のシステム間の内部通信を仲介制御する。これは303システム間内部通信制御部で実現する。前記内部通信は全く外部に対して情報を発信しないため、実際に複数の計算機間で通信をすることに比べ、その通信内容が盗聴されたりすることは少なく安全性が高い。また通信用インタフェースがシステムから見えるのみなので、多重システム並列動作カーネル(300)の構造が分からない限り、その通信内容を解読される可能性も少ない。更に必要に応じて、システム間の通信でアクセス制限を設定する事も可能である。例えば、システム1(201)とシステム2(202)で通信を行う場合、システム2(202)からの要求とその応答のみの通信を許可し、システム1(201)からの通信要求は無視するような設定を施すことも可能である。もし上記アクセス制限を設定した場合、システム1(201)からアクセス制限の不正があった場合や、不正な侵入者によりシステム1(201)上で不正な操作/制御などが行われることをシステム2(202)側で検知した場合、304汎用システム起動終了制御部を通じ、計算機(100)を起動した状態で、システム1(201)の終了や再起動を行うことも可能となる。

【0019】以上の説明で分かる通り、図1の様な構成を取ることで、計算機上で動作するシステムに対し不正な侵入者が不正な操作/制御を行った場合にも、常に安全性の高い対応が可能になる。

【0020】次に本発明の一使用例を図2から図4で説明する。ただし、これはあくまでも一使用例であり、同様な構成を取ることで様々のセキュリティ効果を生むことは可能である。

【0021】図2は、現在一般的に使用されているインターネット、イントラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークにおいて、前記公共回線上のクライアントから特定サイト内へアクセスをする際の通信制御の構成を示した図である。

【0022】図2の構成内容について説明を行う。1000は外部クライアント計算機。1001は外部クライアント計算機(1000)の通信を行うためのインタフェースハードウェア。一般的な例として、LANボード/カード、モデム等が挙げられる。1002は外部クライ

アント計算機(1000)上で稼働するシステム。1003は前記システム(1002)上で動作するクライアントソフトウェアである。2000は前記クライアントソフトウェア(1003)の要求/返答パケットの通信路である、公衆回線。3000は前記クライアントソフトウェア(1003)が要求/返答パケットを送り先である特定サイト。例として企業の内部ネットワークで閉じられたネットワークサイトが挙げられ、前記サイトは公衆回線(2000)と企業内の内部ネットワークのアクセスポイントの両方を保持する。3100は特定サイト(3000)内にある公衆回線(2000)と特定サイト(3000)内の内部ネットワークの中間に位置するセキュリティ用ネットワークで、一般的には境界ネットワークと呼ばれる。3110は、公衆回線(2000)と境界ネットワーク(3100)の間にあり、互いのネットワークを行き来する通信パケットのフィルタリングを行う情報機器で、一般的には外部ルータと呼ばれる。3111は外部ルータ(3110)で、実際にパケットのフィルタリング機能を提供する外部<->境界通信制御部。3120は境界ネットワーク(3100)上に有り、クライアントソフトウェア(1003)からの通信の正当性確認や認証を行う境界サーバ計算機。3121は境界サーバ計算機(3120)の通信を行うためのインタフェースハードウェア。3122は境界サーバ計算機(3120)上で稼働するシステム。3123は前記システム(3122)上で動作するサーバソフトウェアであり、境界サーバと呼ばれる。3124は前記境界サーバ(3123)上で、クライアントソフトウェア(1003)からの通信の正当性確認や認証を行い、必要により特定サイト(3000)の内部ネットワークに処理パケットを送信するクライアント指定処理対応部。3200は特定サイト(3000)内の内部ネットワーク。3210は境界ネットワーク(3100)と内部ネットワーク(3200)の間にあり、互いのネットワークを行き来する通信パケットのフィルタリングを行う情報機器で、一般的には内部ルータと呼ばれる。3211は外部ルータ(3210)で、実際にパケットのフィルタリング機能を提供する内部<->境界通信制御部。3220は内部ネットワーク内にあり、内部ネットワーク(3200)内のクライアントなどの処理や、境界サーバ計算機(3120)上のクライアント指定処理対応部(3124)からの処理を受けて内部処理などを実行する内部サーバ計算機。3230は内部ネットワーク(3200)内の内部クライアント計算機。なお本発明では説明を簡単にするため、計算機を極めて少ない構成で書いたが、実際の場合同じ様な役割を果たす多くの機器が存在する。

【0023】次に図3を使って、外部クライアント計算機(1000)が、特定サイト(3000)内の内部ネットワーク(3200)へアクセスする場合の通信処理流れを説明する。4000で処理が開始される。4001で、

外部クライアント計算機(1000)上のクライアントソフトウェア(1003)が、特定サイト(3000)への処理要求パケットを発行する。前記処理要求パケットの最終的な宛先は、内部ネットワーク(3200)上の内部サーバ計算機(3220)や内部クライアント計算機(3230)なのだが、実際に発行されるパケット要求先は境界ネットワーク(3100)上の境界サーバ計算機(3120)である。4002で、外部クライアント計算機(1000)が発行した処理要求パケットが公共回線(2000)経由で外部ルータ(3110)に送られてくる。4003で、外部ルータ(3110)内の外部<->境界通信制御部(3111)のパケットフィルタリングが行われ、宛先やパケット種別が判断され正当性が確認された処理要求パケットは、境界サーバ計算機(3120)に送られてくる。ここで、もしパケットの正当性が不正な場合は処理を終了(4010)する。

【0024】4004で、境界サーバ計算機(3120)に届いた処理要求パケットは、境界サーバ計算機(3120)内の境界サーバ(3123)に送られ、クライアント指定処理対応部(3124)によって、パケット内容の確認と送り元の認証が行われ、正当性が確認されると、クライアント指定処理対応部(3124)から新たに内部ネットワーク(3200)へ送るため、パケット変換や必要な認証処理が行われ、内部ルータ(3210)に対しパケットが発信する。ここでも、もしパケット内容の正当性が不正な場合や送り元の認証が失敗した場合は、処理を終了(4010)する。4005で、内部ルータ(3210)内の内部<->境界通信制御部(3211)のパケットフィルタリングが行われ、変換後のパケット種別が判断されたり宛先の確認が行われ、正当性が確認されたパケットは、内部ネットワーク内に送られる。

【0025】一方、パケット種別が不正であったり、宛先確認に失敗すると処理を終了(4010)する。4006で、内部ネットワーク(3200)に到着したパケットは、最終的に処理を実行する内部サーバ計算機(3220)や内部クライアント計算機(3230)に送られ、処理要求が実行される。以上が外部クライアント計算機(1000)が、特定サイト(3000)内の内部ネットワーク(3200)へアクセスする時における、一連の通信処理流れである。

【0026】ここで、図2の構成におけるセキュリティの問題点について述べる。

【0027】一般的に、公共回線(2000)、特定サイトのネットワーク内(3100、3200)を流れるパケットは内容の暗号化等が施されており、比較的盗聴等に遭った場合でも安全に設計されている。しかしながら、境界ネットワーク(3100)上に存在する境界サーバ(3123)のベースとして動作するシステム(3122)は、一般的に流通OSやミドルソフトウェアで構成されており、その内部構造等が解析され易い。また境界サー

バ(3123)の役割としては、外からの情報を処理する他、情報を外部に発信する役目を持つ、必然的にパケットのフィルタリングという意味では、内部ルータ(3210)に比べ、外部ルータ(3110)のセキュリティレベルは低く設定されていることが多い。そのため、外部の不正な侵入者が境界ネットワーク(3100)上の境界サーバ計算機(3120)への不正な侵入を試みたり、不正な解析プログラムを送り込んだりするのが容易である。

【0028】不正侵入されたり不正プログラムを送り込まれた場合、送付されてくる処理要求パケット内容の解析や改竄、更には内部ネットワークへ送るパケットの解析や改竄が実行される。そして最終的に企業内などの内部ネットワークに侵入を許し、機密情報などの漏洩やウイルス等の送り込みが行われ甚大な被害を被ることが多い。無論その対策として、境界ネットワーク(3100)の境界サーバ計算機(3120)上のシステム(3122)を、独自のシステムとして稼働することも可能である。ただし、その場合システム上で動作するサーバを始めとするアプリケーションも全く独自なものを用意する必要があり、汎用性が著しく下がる。

【0029】前記セキュリティ上の問題点を解決するため、境界ネットワーク(3100)上の境界サーバ計算機(3120)に、図1で説明した本発明のシステム構成を適応した場合の構成図を図4に示す。

【0030】図4の構成内容について説明を行う。1000、1001、1002、1003、2000、3000、3100、3110、3111、3120、3121、3122、3122、3123、3124、3200、3210、3211、3220、3230は図2で説明した構成と一緒である。300は図1で説明した多重システム並列稼働カーネルである。3125は、外部クライアント(1000)からの処理要求パケットを一時的に保存するための格納領域であるクライアント指定処理要求保存部。3126は境界サーバ計算機(3120)上で内部サーバ計算機(3220)との通信を行うためのインタフェースハードウェア。3127はクライアント指定処理要求保存部の内容監視と、システム(3122)の不正操作/侵入監視を行う監視システム。3321は内部サーバ計算機(3220)の通信を行うためのインタフェースハードウェア。3222は内部サーバ計算機(3220)上で稼働するシステム。3223は前記システム(3222)上で動作するサーバソフトウェアであり、内部サーバと呼ばれる。3224は監視システム(3127)の指示により、クライアント指定処理要求保存部(3125)から外部クライアント(1000)からの処理要求パケットを取得するクライアント指定処理要求取得部。3225はクライアント指定処理要求取得部から処理要求パケットを受け取り、内部ネットワーク内の指定計算機に処理要求パケットを送るためのクライアン

ト指定処理内部ネットワーク対応部。3226は内部サーバ計算機(3220)上で境界サーバ計算機(3120)との通信を行うためのインタフェースハードウェア。3300は内部サーバ計算機(3220)の通信インタフェースハードウェア(3326)と境界サーバ計算機(3120)の通信インタフェースハードウェア(3126)を結ぶネットワークである、専用ゲートウェイLAN。

【0031】本構成の特徴は、境界サーバ計算機(3120)に、図1で説明した多重システム動作カーネル(300)を採用したところである。前記多重システム動作カーネル(300)は境界サーバ計算機(3120)起動時に、従来と同様なシステム(3122)の他、監視システム(3127)をロードする。これらは図1で説明した、システム割込制御部(301)、システムメモリ空間管理部(302)で実現される。また前記それぞれのシステムは、一台の計算機上で動作しているが、システム(3122)は境界ネットワーク(3100)に、監視システム(3127)は専用ゲートウェイLAN(3300)にと、それぞれ全く別々のネットワークに繋がっている。ハードウェア的にも、それぞれのシステムが管理する通信インタフェースハードウェア(3121、3126)は、他システム側のハードウェア情報を検知出来ないように構成されている。これは図1で説明した、ハードウェア割込制御部(305)で実現される。つまり、一台の計算機上で全く、別々のセキュリティレベルを持つ計算機が独立して混在した環境を構成しているのである。

【0032】監視システム(3127)は、多重システム並列カーネル(300)経由で、定期的にシステム(3122)側を監視する。このため、多重システム並列カーネル(300)は、監視システム(3127)からの通信要求とその返答はアクセスを許可するが、逆のシステム(3122)からの通信要求は受け付けないような設定を施してある。これは図1で説明したシステム間内部通信制御部で実現される。もし、外部クライアント(1000)からの処理要求パケットを、システム(3122)側が受信しているようであれば、監視システム(3127)が専用ゲートウェイLAN(3300)経由で内部サーバ計算機(3220)に指示を送り、内部サーバ計算機(3220)が処理要求パケットを取得し、最終的に内部ネットワーク内の指定計算機に処理要求パケットを送る。

【0033】また、境界サーバ計算機(3120)上のシステム(3122)に不正者が侵入したり、不正プログラム等が送り込まれた場合は、監視システム(3127)が検知し、更に多重システム並列カーネル(300)に不正アクセスを試みられた場合にも、多重システム並列動作カーネル(300)が検知し監視システム(3127)に通知され、監視システム(3127)の指示によりシステム(3122)側の終了/リブートが実行され、その通知が管理者に通知される。これは図1で説明したシステム起動終了制御部(304)により実現される。

【0034】図5に図4の構成を使った外部クライアント計算機(1000)が、特定サイト(3000)内の内部ネットワーク(3200)へアクセスする場合の通信処理流れを説明する。なお、境界サーバ計算機(3120)に処理要求パケットが送られてくるまでの処理は、図3と同様なので、それ以降の説明をここでは行う。5000で処理が開始される。5001で、境界サーバ計算機(3120)に届いた処理要求パケットは、境界サーバ計算機(3120)内の境界サーバ(3123)に送られ、クライアント指定処理対応部(3124)によって、パケット内容の確認と送り元の認証が行われ、正当性が確認されると、クライアント指定処理対応部(3124)からクライアント指定処理要求保存部(3125)に格納される。ここでも、もしパケット内容の正当性が不正な場合や送り元の認証が失敗した場合は、処理を終了(5010)する。5002で、監視システム(3127)が多重システム並列動作カーネル(300)経由で、クライアント指定処理要求保存部(3125)を確認し、処理要求パケットが存在する場合、パケット内容の確認を行い正当なパケットであれば、専用ゲートウェイLAN(3300)経由で、内部サーバ(3223)上のクライアント指定処理要求取得部に、パケット取得の指示を出す。ここでも、もし内容の正当性が不正な場合は、処理を終了(5010)する。5003で、クライアント指定処理要求取得部が、クライアント指定処理要求保存部(3125)から、処理パケットを取得し、そのパケットをクライアント指定処理内部ネットワーク対応部(3225)に送付する。5004でクライアント指定処理内部ネットワーク対応部(3225)が、最終的に処理を実行する内部サーバ計算機(3220)や内部クライアント計算機(3230)に送り、処理要求が実行される。以上が本特許のシステム構成を利用した場合における、外部クライアント計算機(1000)が、特定サイト(3000)内の内部ネットワーク(3200)へアクセスする時における、一連の通信処理流れである。

【0035】以上で本発明の一実施例の説明を終わる。

【0036】

【発明の効果】本発明は、単一計算機上で複数システムを同時並列稼働させる環境を利用し、同時並列稼働しているシステム同士のセキュリティをシステム自体の改造無しに確保する。また、例え1つのシステムに不正な侵入がされた場合でも、侵入されたシステム自身の終了/リブートを実行し、他のシステムへの二次的な影響を防止し、他のシステムに影響を及ぼさないセキュリティの確保が可能である。

【0037】特にインターネット、イントラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークで、前記公共回線上のクライアントから特定サイト内へアクセスをする際の通信制御において、前記通信制御用の中継器のセキュリティ確保が

可能となる。

【図面の簡単な説明】

【図1】 本発明のシステム構成図。

【図2】 現在の公共回線越え通信制御の構成図。

【図3】 現在の公共回線越え通信制御処理の流れ図。

【図4】 本発明を公共回線越え通信制御に用いた場合の構成図。

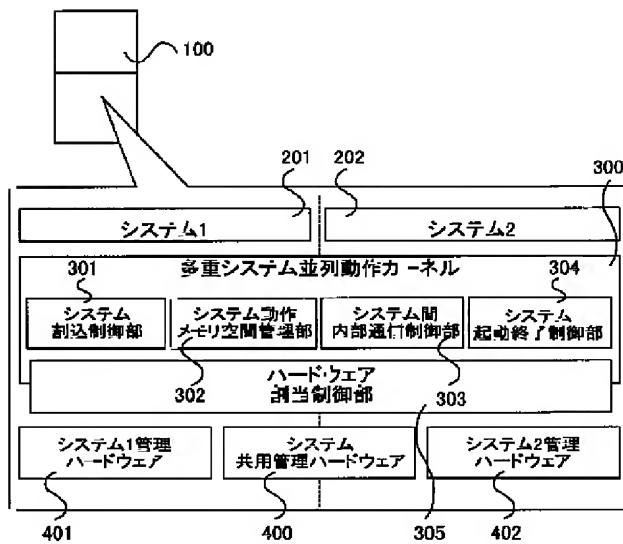
【図5】 本発明による公共回線越え通信制御処理の流れ図。

【符号の説明】

100…計算機、201…システム1、202…システム2、300…多重システム並列動作カーネル、301…システム割込制御部、302…システム動作メモリ空間管理部、303…システム間内部通信制御部、304…システム起動終了制御部、305…ハードウェア割込制御部、400…システム共用管理ハードウェア、401…システム1管理ハードウェア、402…システム2管理ハードウェア。

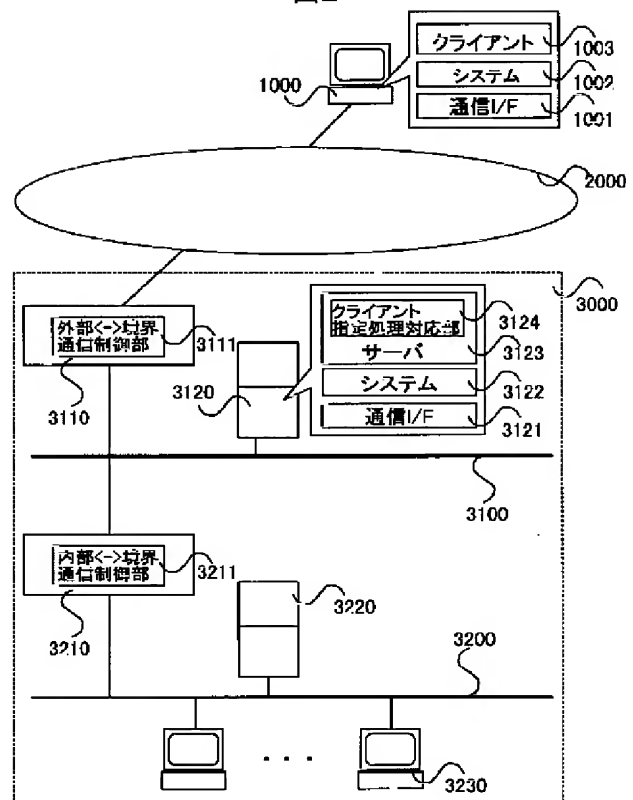
【図1】

図1

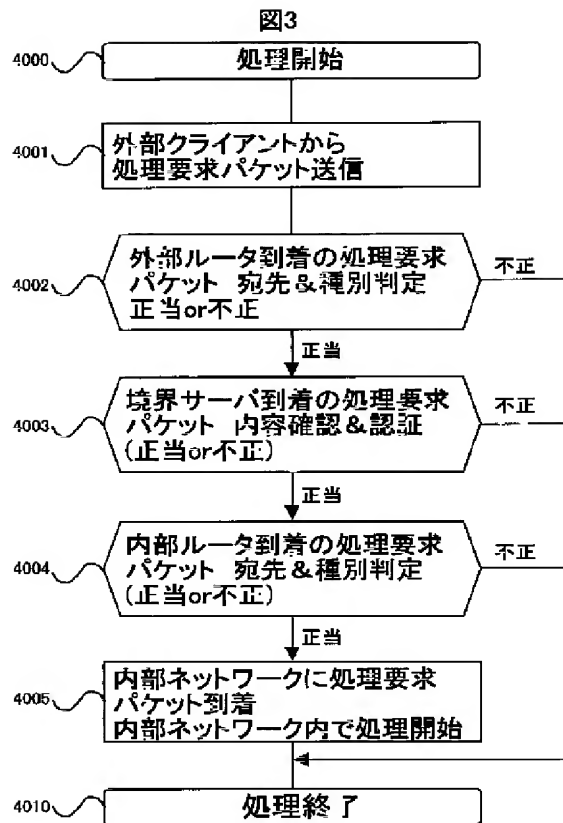


【図2】

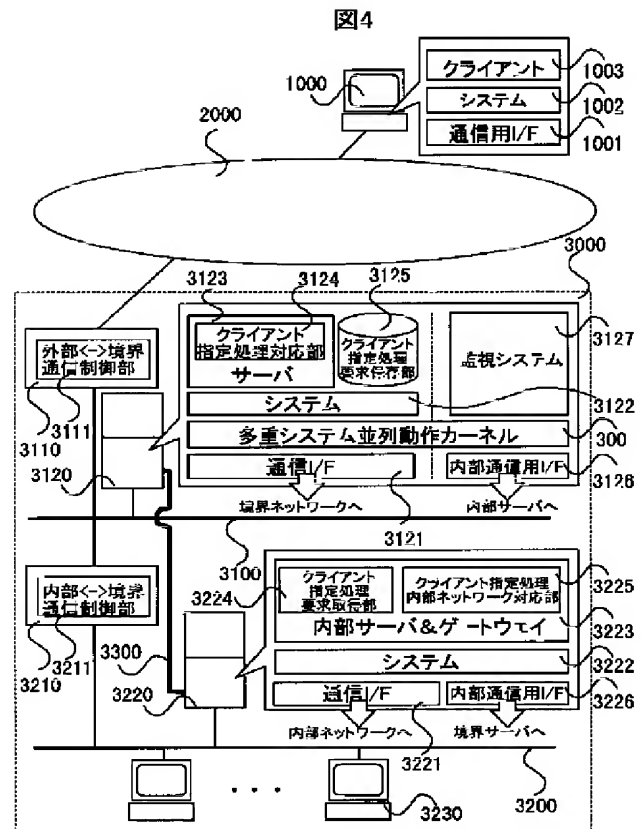
図2



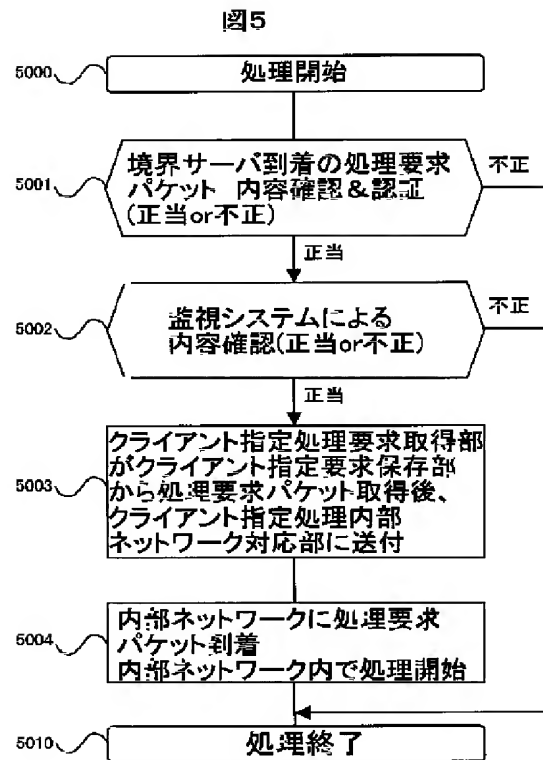
【図3】



【図4】



【図5】



フロントページの続き

(72)発明者 大島 訓
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内
(72)発明者 内山 靖文
神奈川県横浜市戸塚区戸塚町5030番地 株
式会社日立製作所ソフトウェア事業部内

Fターム(参考) 5B017 AA01 BA06 BA07 BB03 CA15
CA16
5B085 AE06 BG07
5B089 GA21 HA10 JB16 JB22 KA17
KB13 KC52 KC58 ME12